



Position Description

Level 2 Network Engineer – Advisory Services (3–5+ Years Experience)

Location: Chicagoland (Hybrid / On-Site as Needed)

Company: 7 Layer Solutions Inc.

Date Revised: August 12, 2026

Reports to: Director / Manager, Advisory Services

About 7 Layer

7 Layer is a Chicago-based technology advisory and cybersecurity firm built around accountability, real-world execution, and long-term client partnerships. We operate at the intersection of IT infrastructure, cybersecurity, compliance, and business strategy—helping organizations build secure, scalable environments that support growth. Our Advisory Services team works on high-impact assessments, redesigns, and transformation projects. We move fast, take ownership, and expect our engineers to think like consultants, not just technicians.

Role Overview

We are looking for a Network Engineer (3–5+ years' experience) to join our Advisory Services & Projects team. This role is focused on network assessments, client advisory, security-driven design, and project implementation—not standard help-desk or ticket-driven support. You will work directly with business owners, IT leaders, and security teams to evaluate real-world environments, identify risk, and lead infrastructure improvements across the Chicagoland market. This is an ideal role for someone ready to grow out of pure support work and into true engineering and consulting.

What You'll Be Doing

- Lead network and security assessments across client environments; identify risk, performance gaps, and security exposures
- Build remediation roadmaps, project scopes, and statements of work
- Design and implement network refreshes and upgrades, firewall replacements, wireless redesigns, and security improvements
- Configure and deploy enterprise-grade networking and security platforms including:
 - Cisco Meraki (Firewalls, Switches, Access Points, SD-WAN)
 - Fortinet (Firewalls, Switches, Access Points, FortiSASE concepts)
 - Palo Alto Networks firewalls and related security services
 - SonicWall and other common mid-market firewall platforms
- Design and support VLAN segmentation, secure VPN solutions (site-to-site and client/remote access), NAT, and routing policies
- Partner with cybersecurity and compliance teams on network hardening, Zero Trust / ZTNA initiatives, and segmented security architecture
- Participate in pre-sales technical discovery, solution design, client presentations, and post-assessment reviews
- Produce clean network diagrams, assessment reports, and high-quality project documentation
- Incorporate modern concepts such as SD-WAN, SASE principles, and cloud networking (Azure VNets / AWS VPCs, cloud firewalls/gateways) into designs where appropriate

What We're Looking For (Required)

- 3–5+ years of hands-on network engineering experience (MSP or consulting experience strongly preferred)
- Strong practical experience with Meraki and Fortinet platforms

- Solid understanding of TCP/IP, DNS, DHCP, VLANs, routing, NAT, IPSec & SSL VPNs, and network security fundamentals
- Experience with network assessments, project delivery, and client-facing technical work
- Ability to produce clear diagrams and written documentation for both technical and non-technical audiences

Nice to Have

- CCNA, PCNSA, PCNSE, or equivalent certifications
- Wireless design and advanced troubleshooting experience
- Exposure to network monitoring / traffic analysis tools and modern observability platforms
- Familiarity with Azure/AWS cloud networking and hybrid connectivity patterns
- Experience in compliance-driven environments (SOC 2, HIPAA, PCI-DSS, etc.)
- Understanding of Zero Trust Network Access (ZTNA) and SASE concepts

Please note this job description is not designed to cover or contain a comprehensive listing of activities, duties, or responsibilities that are required of the employee for this job. Duties, responsibilities, and activities may change at any time with or without notice.